AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for providing identification authentication, comprising:

receiving an identification credential from an individual, including a biometric data, wherein the identification credential is an identification card, wherein the biometric data is stored on the identification credential, and wherein the identification credential is digitally signed with a private key;

receiving a biometric sample from the individual;

validating the digital signature using a corresponding public key;

determining if a difference between the digitally signed biometric data and the biometric sample from the individual is below a predetermined threshold; and

providing the results of the determination to an interested party;

whereby the identity of the individual is authenticated with reference to the identification credential alone, without having to transmit information for the individual over a network.

2. (Original) The method of claim 1, further comprising adjusting the predetermined threshold in accordance with instructions received from a user.

3. (Previously presented) The method of claim 1, wherein the identification credential includes at least one of a name, a unique ID, a citizenship,

an issue date, an expiration date, an identifier for an issuing authority, the biometric data, and a digital photo.

4. (Previously presented) The method of claim 1, wherein the biometric sample includes one of, or a combination of, a fingerprint, a signature, an iris scan, a facial scan, a voice pattern, a height, a weight, or a palm scan.

5. (Original) The method of claim 1, wherein the digitally signed biometric data is contained in a magnetic stripe, a bar code, a smart card, a chip-card, or a non-volatile memory, such as flash memory, located on or within the identification credential.

6. (Original) The method of claim 1, wherein the digital signature is provided by a central certification authority.

7. (Original) The method of claim 1, further comprising granting access to resources based on the determination if the difference between the digitally signed biometric data and the biometric data from the individual is below the predetermined threshold.

8. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for providing identification authentication, the method comprising:

receiving an identification credential from an individual, including a biometric data, wherein the identification credential is an identification card, wherein the biometric data is stored on the identification credential, and wherein the identification credential is digitally signed with a private key;

receiving a biometric sample from the individual;

validating the digital signature using a corresponding public key;

determining if a difference between the digitally signed biometric data and the biometric sample from the individual is below a predetermined threshold; and

providing the results of the determination to an interested party;

whereby the identity of the individual is authenticated with reference to the identification credential alone, without having to transmit information for the individual over a network.

9. (Original) The computer-readable storage medium of claim 8, wherein the method further comprises adjusting the predetermined threshold in accordance with instructions received from a user.

10. (Previously presented) The computer-readable storage medium of claim 8, wherein the identification credential includes at least one of a name, a unique ID, a citizenship, an issue date, an expiration date, an identifier for an issuing authority, the biometric data, and a digital photo.

11. (Previously presented) The computer-readable storage medium of claim 8, wherein the biometric sample includes one of, or a combination of, a fingerprint, a signature, an iris scan, a facial scan, a voice pattern, a height, a weight, or a palm scan.

12. (Original) The computer-readable storage medium of claim 8, wherein the digitally signed biometric data is contained in a magnetic stripe, a bar code, a smart card, a chip-card, or a non-volatile memory, such as flash memory, located on or within the identification credential.

13. (Original) The computer-readable storage medium of claim 8, wherein the digital signature is provided by a central certification authority.

14. (Original) The computer-readable storage medium of claim 8, wherein the method further comprises granting access to resources based on the determination if the difference between the digitally signed biometric data and the biometric data from the individual is below the predetermined threshold.

15. (Currently amended) An apparatus for providing identification authentication, comprising:

a receiving mechanism that is configured to receive an identification credential from an individual, including a biometric data, wherein the identification credential is an identification card, wherein the biometric data is stored on the identification credential, and wherein the identification credential is digitally signed with a private key;

a sampling mechanism that is configured to receive a biometric sample from the individual;

a validation mechanism that is configured to validate the digital signature using a corresponding public key;

a determination mechanism that is configured to determine if a difference between the digitally signed biometric data and the biometric sample from the individual is below a predetermined threshold; and

a feedback mechanism that is configured to provide the results of the determination to an interested party;

whereby the identity of the individual is authenticated with reference to the identification credential alone, without having to transmit information for the individual over a network.

16. (Original) The apparatus of claim 15, further comprising an adjustment mechanism configured to adjust the predetermined threshold in accordance with instructions received from a user.

17. (Previously presented) The apparatus of claim 15, wherein the identification credential includes at least one of a name, a unique ID, a citizenship, an issue date, an expiration date, an identifier for an issuing authority, the biometric data, and a digital photo.

18. (Previously presented) The apparatus of claim 15, wherein the biometric sample includes one of, or a combination of, a fingerprint, a signature, an iris scan, a facial scan, a voice pattern, a height, a weight, or a palm scan.

19. (Original) The apparatus of claim 15, wherein the digitally signed biometric data is contained in a magnetic stripe, a bar code, a smart card, a chip-card, or a non-volatile memory, such as flash memory, located on or within the identification credential.

20. (Original) The apparatus of claim 15, wherein the digital signature is provided by a central certification authority.

21. (Original) The apparatus of claim 15, further comprising a security mechanism configured to grant access to resources based on the determination if the difference between the digitally signed biometric data and the biometric data from the individual is below the predetermined threshold.